Developing a Secure & High Speed Algorithm for Real-Time Systems

Synopsis

Submitted to

Swami Ramanand Teerth Marathwada University, Nanded.

For the degree of

Doctor of Philosophy in Computer Science

Under

Faculty of Science

By

Ebrahim Abduljalil Khaled Naji

Taiz, Yemen

Under the guidance of

Dr. Suryakant B. Thorat

Principal,
ITM College, Nanded.

School of Computational Science,

S. R. T. M. University, Nanded - 431606.

Developing a Secure & High Speed Algorithm for Real-Time Systems

Synopsis

1. Introduction:

Real-time database systems extend the set of correctness requirements from conventional database systems. Transactions in real-time systems must meet their timing constraints, often expressed as deadlines, in order to be correct.

In stock market applications and automated factories, a poor response time from the database can result in the loss of money and property. The problem of conflicting requirements involves dynamically keeping track of both the real-time and the security aspects of the system performance.

When the system is performing well and making a high percentage of its deadlines, conflicts that arise between security and real-time requirements will tend to be resolved in favor of the security requirements more often, and more priority inversions will occur. However, the opposite is true when the real-time performance of the system starts to degrade. Then, the scheduler will attempt to eliminate priority inversions, even if it means allowing occasional covert channels.

The real-time requirements of a transaction are given by four variables: priority, execution time, release time, and periodicity.

2. Review of Literature:

There are many proposals that studied the Real-Time systems and security issues in the literatures. We briefly review some of them below.

In [10], authors present the secure two phase locking protocol and discuss an adaptive method to support trading off security for timeliness, depending on the current state of the system. The performance of the adaptive secure two-phase locking protocol shows improved timeliness. they also discuss future research direction to improve timeliness of secure database systems.

They have presented an approach to scheduling transactions to improve timeliness in a secure real-time database.

The work described is more a direction for future research than a concrete solution to the problem of secure real-time concurrency control.

Authors have considered a simple trade-off between deadline miss percentage and security.

In [11], a novel buffer management algorithm SABRE provides covert-channel-free security. SABRE employs a fully dynamic one-copy allocation policy for efficient usage of buffer resources. It also incorporates several optimizations for reducing the overall number of killed transactions and for decreasing the unfairness in the distribution of killed transactions across security levels. And using a detailed simulation model, the real-time performance of SABRE is evaluated against unsecure conventional and real-time buffer management policies for a variety of security classified transaction workloads and system configurations.

Their experiments show that SABRE provides security with only a modest drop in real-time performance. Finally, they evaluate SABRE's performance when augmented with the GUARD adaptive admission control policy. Their experiments show that this combination provides close to ideal fairness for real-time applications that can tolerate covert-channel bandwidths of up to one bit per second (a limit specified in military standards).

In [20], a novel adaptive approach for security support is proposed in which a Real-Time Embedded Systems (RTESs) initially uses a relatively short cryptographic key to maximize the QoS, while increasing the key length when the security risk level is raised. can make a possible cryptanalysis several orders of magnitude harder by requiring the attacker to search larger key space, while meeting all deadlines by degrading the QoS in a controlled manner. To minimize the overhead, they derive the appropriate QoS

In [21], identified the covert channel property of secure real-time databases and, we have proposed a new secure optimistic concurrency algorithm based on this property. They have implemented the secure algorithm and a non-secure algorithm and studied their performance in detail using a real-time database system simulation model.

Results show that the algorithm performs fairly well in terms of security and timeliness compared to a non-secure algorithm. They argue and show that achieving more security does not necessarily mean more sacrifice in real-time performance.

Most secure DBMS attempt to achieve the secrecy objective by incorporating access control mechanisms based on the well-known Bell–LaPadula model. This model is specified in terms of subjects and objects. An object is a data item,

whereas a subject is a process that requests access to an object. Each object in the system has a classification level (e.g., Secret, Classified, Public, etc.) based on the security requirement. Similarly, each subject has a corresponding clearance level based on the degree to which it is trusted by the system.

The real-time protocols: 2PL-HP , which is based on locking, and OPT-WAIT , which is based on optimistic concurrency control. Both these protocols are completely free from priority inversion and can therefore be used to resolve conflicts in an RTS.

3. Problem Statement

In most of Real-Time systems, there is an amount of data to be consulted, processed and updated, and while doing so the database consistency should be maintained.

And there are time constraints associated with various operations; during every stage of the bidding process, data security must be ensured — unauthorized access to the secret information by bidders may help them gain unfair and financially lucrative advantages over other competitors.

The Real-Time system has to satisfy two requirements in the same time, namely, provide security and minimize the number of killed transactions.

In those systems, high priority is usually given to transactions with earlier deadlines in order to help their timely completion. On the other hand, in secure Real-Time system, low security transactions are given high priority in order to avoid covert channels.

We will develop an algorithm that can simultaneously and effectively meet the above problems.

4. Research Objectives:

The main objective of this research is to solve the problem described above through the following:

1- To develop an algorithm that achieves security with high speed real-time system.
2- To offer covert channels that achieves a more security and speed in data transferring.
3- Reducing the overall number of killed transactions and decreasing the rate of violation of security.

5. Research Methodology:

To achieve the research objectives, many stages of work need to be executed. It will begin by doing a literature review on Real-Time Security; their methodologies, techniques, pedagogies, tools, and challenges of security in Real-time systems.

Some of the algorithms that providing a quality service, fast delivery and security in real-time systems will be implemented and evaluated.

These stages of work need different resources and tools to be achieved. Labs and various software programs are required beside the digital libraries. The following discusses in more details the suggested stages of study.

Stage 1: Literature Review and Related Work

In this stage, an extensive study will be accomplished in Real-Time systems including its tools, methodologies, pedagogies, techniques and issues, etc and their research challenges. Then, a comprehensive survey of RTS security will be done

Stage 2: Analyzing Real-Time Systems

In this stage, we will analyze the real-time system and it's components, for evaluating the security and performance.

Stage 3: Building the proposed algorithms providing a quality service, fast delivery and security in real-time system (RTS).

According to the milestones of stages 2 and 3, the proposed algorithms that providing a quality service, fast delivery and security in RTS will be developed.

Stage 4: Implementation and evaluation

The proposed algorithms providing a quality service, fast delivery and security in RTS will be implemented and evaluated using the real data by the system.

Figure 1 shows block diagram of work stages and explain the relationship between

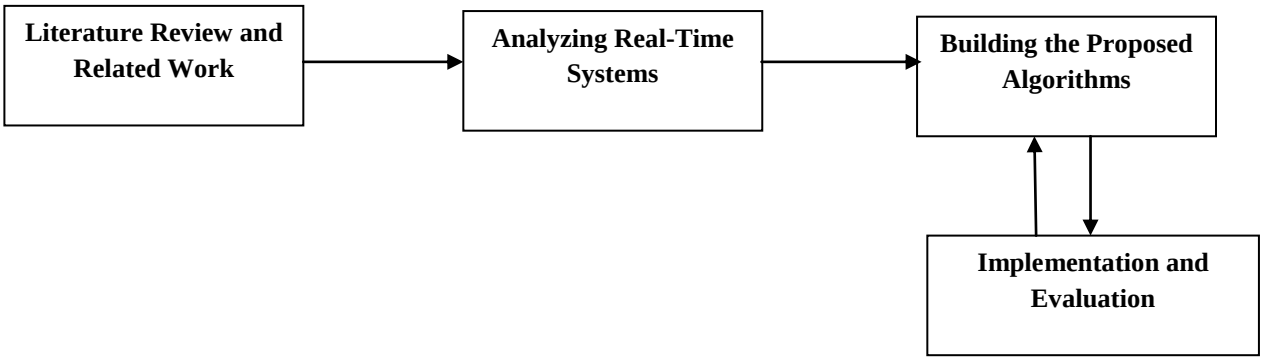

Fig. (1): Block diagram of work stages.

References:

[1] Quanhua Liu, Yazhou Wang ,Fathy A.E., "*Towards Low Cost, High Speed Data Sampling Module For Multifunctional Real-Time Uwb Rada"r*, Aerospace and Electronic Systems, IEEE Transactions , 2013

[2] Shatabdi Sahaa, S.K.Setuab, *"Extending Trust In Time Dependent Database Systems"*, IEEE- International Conference On Advances In Engineering, Science And Management (lCAESM -2012) March 30, 31, 2012.

[3] Hao Liu, Yaoxue Zhang, Yuezhi Zhou, Xiaoming Fu, Laurence T. Yang," *Receiving Buffer Adaptation for High-Speed Data Transfer*", IEEE TRANSACTIONS ON COMPUTERS, 2013

[4] D. Maxim, M. Houston, L. Santinelli, G. Bernat, R.I. Davis, L. Cucu-Grosjean, *"Re-Sampling for Statistical Timing Analysis of Real-Time Systems*", Real-Time and Network Systems (RTNS), 2012

[5] G. Buttazzo, M. Bertogna, and G. Yao, "*Limited Preemptive Scheduling for Real-Time Systems: a Survey*"**,** IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, pp. 3-15, February 2013.

[6] Po-Wen cheng, che-chou shen, and Pai-chi li, Fellow**,** "*MPEG Compression of Ultrasound RF Channel Data for a Real-Time Software-Based Imaging System*"**,** IEEE TransacTIons on UlTrasonIcs, 2012

[7] Alan Burns·Ian J. Hayes, "*A timeband framework for modelling real-time systems"* ,Springer Science+Business Media, LLC 2010

[8] Rourab Paul, Sangeet Saha, Suman Sau, Amlan Chakrabarti, *"Design And Implementation Of Real Time Aes-128 On Real Time Operating System For Multiple Fpga Communication*"**,** 2008

[9] Dr.S.B.Thorat , S.K.Nayak, M.M.Bokhare, *"Data Security : An Analysis*" , (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010.

[10] Dr.S.B.Thorat, S.K.Nayak, Miss.Jyoti P Dandale, "*Facial Recognition Technology: An analysis with scope in India*", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 1, 2010.

[11] Maysam Hedayati, Seyed Hossein Kamali, Reza Shakerian, Mohsen Rahmani, "*Evaluation of Performance Concurrency Control Algorithm for Secure Firm Real-Time Database Systems via Simulation Model*", 201O International Conference on Networking and Information Technology.

[12] Richard Marquez, Eitan Altman, And Solazver Solé-ۥLvarez, "*Time-Averaging Of High-Speed Data Transfer Protocols*", IEEE, 2005

[13] W. Mao. "*Modern Cryptography*". Prentice Hall, 2004.

[14] Magdalena Dobrzańska, Paweł Dobrzański, Artur Łopuszyński, Łukasz Kurowski "*Using Real-Time System To Manage Production Data In A Distributed System" ,* ACM, 2008

[15] K. D. Kang, S. H. Son., "*Systematic Security and Timeliness Tradeoffs in Real-Time Embedded Systems"*, Technical Report CSTR- 06-KDOI, Department of Computer Science, SUNY Binghamton, 2006

[16] J. Loyall, R. Schantz, D. Corman, j. P. , S. Fernandez, "*A Distributed Real-Time Embedded Application for Surveillance, Detection, and Tracking of Time Critical Targets*", In The 11th IEEE Real-Time Embedded Technology and ApplicatiOns Symposium, 2005.

[17] Binto George, Jayant R. Haritsa, "*Secure Concurrency Control in Firm Real-Time Database Systems*", Journal Distributed and Parallel Databases, Springer 2000.

[18] S. H. Son, R. Mukkamala, R. David, "*Integrating Security and Real-Time Requirements using Covert Channel Capacity*", IEEE Transactions on Knowledge and Data Engineering, 12(6), Dec 2000.

[19] E. Spyropoulou, T. Levin, C. Irvine, "*Calculating Costs for Quality of Security Service*", In 15th Computer Security Applications Conference, 2000.

[20] Kimmel, Ron., "*Three-dimensional face recognition*", Retrieved 2005-01-01.

[21] K. D. Kang, S. H. Son, J. A. Stankovic. "*STAR: Secure Real-Time Transaction Processing with Timeliness Guarantees*", The 23rd IEEE International Real-Time Systems Symposium, Dec. 2002.

[22] Sang H. Son**,** *"Supporting Timeliness and Security in Real-Time Database Systems".*

[23] Victor C. S. Lee, John A. Stankovic, Sang H. Son, *Intrusion Detection in Real-time Database Systems Via Time Signatures*, IEEE 2000.

[24] Denning, D. E., "*An Intrusion-Detection Model"*, IEEE, Transactions on Software Engineering, vol. SE-13, no. 2, pp.222-232, 1987.

[25] Sang H. Son, "*Towards a Multilevel Secure Database Management System for Real-Time Applications*", Bhavani Thuraisingha- The MITRE Corporation, Bedford, MA 01730

[26] Sang H. Son, Craig Chaney, Norris P. Thomlinson, "*Partial Security Policies to Support Timeliness in Secure Real-time Databases",* Dept. of Computer Science, University of Virginia, Charlottesville, VA 22903.

[27] Giorgio C. Buttazzo, "*Hard Real-Time Computing Systems* " (ISBN 978-1-4614-0675-4) (Springer, 2011 — 3rd edition.)

[28] Hermann Kopetz , *"Real-Time Systems*", (ISBN 978-1-4419-8236-0), (Springer, 2011 — 2nd edition.)

[29] Giorgio C. Buttazzo, Giuseppe Lipari, Luca Abeni and Marco Caccamo **,** *"Soft Real-Time Systems: Predictability vs. Efficiency"* (ISBN: 978-0-387-23701-5), (Springer, 2005.)

[30] Albert M. K. Cheng, *"Real-Time Systems: Scheduling, Analysis, and Verification"*, (ISBN: 978-0-471-18406-5), (John Wiley & Sons, 2002.)

[31] Alan Burns and Andy Wellings, *" Real-Time Systems and Programming Languages"*, (ISBN: 0201729881), (Addison Wesley Longman, 2001 — 3rd edition.)

[32] Alan C. Shaw, *"Real-Time Systems"*, (ISBN: 978-0-471-35490-1), (John Wiley & Sons, 2001.)

[33] Jane W. S. Liu, *"Real-Time Systems"*, (ISBN: 0130996513), (Prentice Hall, 2000.)

Ebrahim A. Naji
Research Scholar

Dr. S. B.Thorat
Research Guide